IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 8 Issue 2, February 2021
ISSN (Online) 2348 – 7968 | Impact Factor (2020) – 6.72
www.ijiset.com

# Investigation of Techniques used for Mitigating Security and Privacy Issues in Cloud Based Electronic Health Record (EHR) Systems

**Vidhi Thakkar [1] and Dr. Vrushank Shah[2]**

[1] FCAIT Department, GLS University, Ahmedabad, Gujarat, India

[2] HEAD EC Department, Indus University, Ahmedabad, Gujarat, India
vidhi@glsica.org

**Abstract**

Recently, many healthcare organizations have started adopting intelligent cloud-based EHR (Electronic Health Record) applications due to improved technological innovations. Integrating cloud services with healthcare systems provide benefits such as scalable, flexible, reliable, and cost-effective environment for easy sharing of health records between healthcare providers and stakeholders. However numerous benefits inherited from cloud computing to the healthcare organizations, security and privacy concerns are still hindering its wide adoption. Security and privacy preservation of healthcare data are mandatory considering the sensitivity of data involved in this sector. Over the past few years, several attempts have been made to provide a secure and reliable EHR framework. But the model still suffers from various security and privacy attacks due to the lack of transparency, trust, and dynamic nature of EHR applications. This paper aims to analyze existing security and privacy preservation approaches with their limitations, security and privacy threats of cloud-based EHRs, and envisioned future research directions.

***Keywords:*** **Electronic Health Records (EHR), Cloud Computing, healthcare, data privacy and security, threats, privacy preservation, transparency, authentication.**

## 1. Introduction

Digital technology is changing the aspect of the healthcare system across the world. To support these changes, many healthcare service providers are outsourcing cloud services for maintaining healthcare records. This evolution has converted paper-based records into electronic health records (EHRs). According to HealthIT.gov report [2], office-based physician adoption of any EHRs in 2017 has more than doubled since 2008, from 42\% to 86\%. By adopting cloud technology, the cloud service providers can offer several benefits such as pay-per-use, fast, cost-effective, scalable, and flexible infrastructure. According to a Market Data Forecast report, the acquisition of cloud computing technology is increasing in the global cloud computing market. The size is forecasted to grow from USD 371.4 billion in 2020 to USD 832.1 billion by 2025 [4].

EHR is a digital form of a patient's paper-based records. Integrating EHRs with cloud computing technology builds up a patient-centric system and makes medical records available instantaneously to the stakeholders [1]. EHR contains patient medical history, diagnoses, prescriptions, treatments, allergies, and reports. EHR helps healthcare organizations for generating a reliable progression of information within digital care infrastructure. Which helps in effective patient care, decreases health care costs, and predicts outbreaks of epidemics [10]. Although cloud-based EHRs provide easy access and transference of patient records to users, EHR records are insecure on cloud networks and vulnerable to various security and privacy attacks. The cloud service provider stores patient private-sensitive data remotely, which provides attackers the one-stop center to intercept and counterfeit the health record during the transmissions. By storing healthcare data on a third-party server, makes it difficult for the patients to control their data and throws unique challenges related to the privacy and security of healthcare information [5] [6] [7].

Various security and privacy concerns such as data confidentiality, access control, integrity, cybersecurity issues, interoperability, accountability are faced in cloud-based EHR systems [6] [27]. Additional privacy concerns emerge from the widespread dispersal of data throughout the healthcare system without explicit patient consent [31]. EHRs are also

vulnerably misused by the insiders of the healthcare organization for personal or economic gain [29]. Healthcare organizations accumulate patient information for a legitimate purpose but, barely any controls exist to guarantees that it isn't revealing the patient's privacy. Hence, a need arises to implement a secure and dynamic mechanism to confine access to patient information based on risk analysis [7] [8] [22].

Numerous strategies have been implemented by cloud service providers to address the security and privacy concerns in EHRs. The most widely utilized approaches are encryption, trust establishment (digital signatures), access controls, secure channels, data anonymization, and auditing. However, there exists a gap in the empirical use of cloud-based EHR services by the users due to insufficient infrastructure, accountability, and transparency to provide after-the-fact reviews for unusual human behavior [9] [28].

This study aims to review the existing approaches for maintaining the privacy and security of cloud-based EHRs with their limitations. We also have analyzed various security and privacy threats that restrict the successful implementation of cloud-based EHRs within healthcare organizations.

This paper is divided into the following sections: section two describes security and privacy concerns for EHRs. Section three describes the security and privacy requirements for adopting cloud computing infrastructure in healthcare organizations. In section four, we analyze security and privacy-preserving mechanisms used to secure healthcare records. Section five discusses the security and privacy threats of cloud-based EHRs. Finally, in section six, we have given a comparative analysis of existing frameworks and also pointed out some open research challenges, and section seven gives overall conclusions of this research effort.

## 2. Background

EHR records are exchanged between multiple organizations for providing the best care to patients and improve the efficiencies of healthcare organizations. However, this distributed setting of EHR records increases substantial concern regarding patient privacy disclosure to unauthorized users while transmitting them over the network.

### 2.1 Security and Privacy in Cloud-Based EHR

Security and privacy are the primary concern for healthcare organizations due to the sensitivity of the data involved. Security and privacy concerns are increasing year-by-year thus must be addressed seriously. Data security is concerned with the protection of data from unauthorized users. Privacy defines rules and regulations for controlling access to a patient's sensitive data only to the authorized entities. Data ownership is related to patient data privacy and states that the patient has the privilege to control how his private records to be accessed by authorized stakeholders. Security is not related to ownership but plays a crucial role in accessing healthcare data due to increasing digital dependency [3] [6] [10].

Differentiating security and privacy is confusing as they overlap. Privacy concerns indirectly cover most of the security concerns. For example, to preserve privacy, it is necessary to address security issues like authentication, non-repudiation, fine-grain access control policy, availability, accountability, and transparency [27]. Security protects healthcare records from being vulnerable to unauthorized access, modification, and demolition [10].

### 2.2 Laws and Regulations for Preserving Patient Privacy

Cloud computing demands strict adherence to laws, regulations, and legal frameworks for preserving the privacy of healthcare data. Healthcare providers have to follow these standards while exchanging health records among various stakeholders. Many medical government institutions have developed a framework to ensure security and privacy for cloud-based applications. Many countries such as United States, Canada, UK, Russia, India, and Brazil have data protection regulations and laws. Different privacy regulations such as Health Insurance Portability and Accountability Act (HIPAA),

Personal Information Protection and Electronic Documents Act (PIPEDA), and the Indian EHR standard protect health records from threats [15]. According to this legislation, a patient has the right over his private medical records and can set rules and limits on who can look at and receive his health information [5][10]. A violation of these laws has serious implications for any healthcare practitioner or facility [6].

### 2.3 Past Attacks in Healthcare

As healthcare gets digitized with millions of health records produced every day, healthcare providers must consider any inside or outside threats. Every year an immense number of data breaches are reported making it difficult for an individual to count. Malicious opponents are continuously finding a new path to enter cloud storage to steal sensitive information. EHR data breaches can have a devastating impact on an entire nation as many healthcare sectors are inter-linked with the government [11].

According to the Info Security Magazine report, "More healthcare records were breached in 2019 than in the six years from 2009 to 2014" [12]. Over a while, attackers have created various high-tech methodologies to steal users' credentials, leading to an unavoidable threat. Unauthorized access and disclosure are the crucial types of breaches occurring in the healthcare organization. As a report stated by ZDNet Cybersecurity in 2019, some researchers have found phishing campaigns having the intent of stealing user credentials from government departments across the globe [13].

The Healthcare sector is more vulnerable to insider threats compared to outsider threats. According to HIPPA Journal Report [14], data breach incidents caused by insiders is 59\% which is 17 \% more than outsider threats. It is difficult to estimate the harm caused to patients and healthcare organizations through data breaches. For better healthcare, individuals must ensure that patient health information is private and secure. Otherwise, a patient will not disclose his sensitive data to the healthcare providers and which cloud diminishes EHR adoption [15].

### 2.4 Cloud-based EHR Security and Privacy Concerns

Cloud-based EHR provides significant advantages to patients and healthcare organizations however it brings several concerns related to privacy, confidentiality, and security of healthcare information for both of them.

Concerns over the privacy and security of EHR fall into three categories:

(1) Concerns about unauthorized access of information from insiders of an organization.

(2) Concerns about misuse or alteration of health information from an attacker while transmitting over the network.

(3) Concerns of misuse of data when knowing or unknowingly shared by healthcare organizations to the government agencies for medical research.

Data security and privacy concerns are the biggest hindrances to the success of EHR applications [6]. Though communication technology permits the usage of advanced technical strategies to control access to a patient's private health information, it brings new breaches.

### 2.5 Patient Concerns

Healthcare data is a valuable asset of a patient. On the other side, sharing them is vitally essential for intelligence healthcare services. Patients' trust in EHRs can be acquired only when they have an assurance that the healthcare organizations preserve their sensitive records as per the stated privacy document [5] [22]. The patient should have access to his information and can control other stakeholders of the healthcare system.

The trust deficit between the healthcare organization and its users can be minimized by making the patient owner of his information and rights to control other stakeholders in the healthcare system. It can help healthcare professionals to full access to information for better diagnosing diseases. Healthcare providers should implement a transparent and accountable system where patients, administrators, and the system can detect unauthorized access and prevent potential medical disputes. Transparency helps patients to monitor any deviations happening on their data and can revoke user's further access on time [9] [28].

## 3. Security and privacy requirements of the cloud-based EHR systems

EHRs in the cloud servers are not reliable without accomplishing security and privacy measures. Security and privacy requirements assist in preventing unauthorized use of data and protect against loss and tampering [5-7] [16] [22] [28] [31] [32].

Cloud-based EHR security and privacy requirements:

1) Authenticity: It ensures only the authorized and authentic authority can access sensitive health records.

2) Confidentiality: It ensures that sensitive information of a patient is prevented from unauthorized access and is only accessible by the authorized entities. Also, patient privacy is protected when liaising with external agencies.

3) Data integrity: It ensures that the patient's records are accurate and have not been altered by either authorized or unauthorized users in any way.

4) Availability: It ensures that healthcare information is available in any critical situation.

5) Non-repudiation: It ensures that the patients or the doctors cannot deny after pilfering the health data.

6) Accountability: It ensures any embezzlement to the records by authorized or unauthorized users is identified in the EHR system.

7) Privacy: It ensures that the patient's information is protected not used for any other purpose.

8) Anonymity: It ensures that the patient's identity and private information remain anonymous when an outsider tries to obstruct their data during transmission or storage.

9) Consent Exception: Consent exception allows access to health records of a patient in an emergency case to the specified users (doctors or relatives of a patient’s). Inability or prevention of the access rules may threaten a patient’s life.

10) Data Ownership: Authority should be given to the patient to decide who can access his health data.

11) Behavior-based Tracking and revocation of access rights: A system or patient should be able to recognize fraudulent transactions and revoke further access rights. A patient must be given control for revoking the rights of other stakeholders if he found any deviations.

12) Adaptive Access Control Policy: The access control policy should be dynamic and adaptive and takes access control decisions by measuring the amount of risk when users access data.

Achieving security and privacy requirements for cloud-based EHRs is vital as exchanging them may prompt different attacks.

## 4. Existing mechanism for maintaining privacy and security of healthcare records in the cloud-based environment

Security and privacy of the patient's records is the significant concern while outsourcing EHRs on a centralized cloud-based system. Several approaches have been proposed to preserve the privacy and security of healthcare data. Following are the most commonly used techniques for addressing the security and privacy issues for healthcare data with respect to cloud computing.

### 1) Encryption:

Encryption is the most prominent method to ensure data confidentiality. It keeps health information secret while transmitted over a network. There are three types of encryption/decryption techniques [17] [18]. The first one is a symmetric-key algorithm that shares the same secret key for both encryption and decryption. The most common symmetric key algorithms are AES, DES, 3DES, BLOWFISH, and RC4. The symmetric encryption algorithms are fast but unable to provide sufficient security for healthcare records due to incompatibility with role-based encryption. The second type of encryption algorithm is the asymmetric-key algorithm that uses a pair of related keys- a public key and a private key for encryption and decryption. Examples of them are RSA, DSA, Elliptic curve cryptography, Diffie-Hellman key exchange, EI-Gamal. While Comparing to Symmetric key algorithms, asymmetric algorithms provide confidentiality, authenticity, integrity, and non-repudiation to data transmission and storage. Hybrid encryption combines the advantage of symmetric and asymmetric encryption, makes a more robust system. The third technique is hashing, which ensures the integrity of data. Hashing has algorithms like MD5, MD6, SHA, and SHA256 [3] [8]. There are several parameters used for the measurement of encryption/decryption algorithms. Such as key length, block size, file size, no. of rounds, encryption/decryption time, confidentiality, memory usage, and cost [19].

There are various encryption algorithms available however it is important to implement the right algorithm to secure data. For better effectiveness, authors are also combining symmetric and asymmetric encryptions. For example, the authors of [35] proposed a hybrid model by combining three different encryption techniques for securing sensitive data in the cloud environment. The model was secure enough against most of the security attacks. The hybrid algorithm had three security policies for assuring complete security to the data while storing, processing, and accessing them. In addition, the authors of [20] designed homomorphic encryption for cloud computing security by performing calculations on encoded data in the cloud server without knowing the raw data. The novel and secure MRS algorithm (modified RSA) requires a short time for encryption and reduces the redundancy in messages. Cryptographic approaches are sufficient only for protecting the information which is stored on the cloud. However, EHR services require data transmission over communication systems and where an unauthorized user can alter, theft, or snoop system data. These encryption approaches are not capable of detecting points when an illegitimate user has performed any unauthorized modifications. Encryption approaches could not guarantee absolute security against any technical attacks [8].

**2) Authentication:**

Authentication assures that healthcare information is accessible only to authorized users. There are three types of authentication factors available in cloud network security: single-factor authentication (SFA), two-factor authentication (2FA), and multi-factor authentication (MFA). Single-factor authentication is the conventional and the simplest type of authentication technique. SFA uses passwords for security and which can be easily cracked by hackers. Therefore, not sufficient to secure sensitive healthcare information [8]. Healthcare organizations have started to use 2FA to increase the security of their records. 2FA uses a one-time password for the confirmation of user identity. However, there is a possibility of OTP generation device theft or loss. OTPs sent on mobile phones are also not secure since an unauthorized user can thieve a user's mobile or hack SMS and email [21].

Another authentication scheme is MFA that combines two or more independent authentication factors such as passwords, biometrics, smart cards, security tokens, etc. The password is the oldest and foremost authentication factor in the information security world. However, transmitting the password in the secure protocol communicating entities over the cloud exacerbates the security issues. Smart cards are more secure for storing and transporting medical history. But, not feasible for EHR applications. A biometric authentication system performs validation on an individual's unique biological characteristics to permit access and is in demand. Multi-factor offers greater security to cloud data but, they are difficult for healthcare organizations since they have to maintain acceptable efficiency levels. They are challenging to implement due to the high cost of integration [22] [23].

As healthcare organizations operate in a unique environment, the challenge is to perform continuous authentication on practitioner. For example, the authors [22] proposed a framework with three components: adaptive authentication, risk analysis, and data transparency. The adaptive authentication assesses the amount of risk in user data. Data transparency helps patients, administrators, and the system to identify and detect deviation from patient consent.

**3) Access Control:**

Access control is the primary security component to control data breaches from insider attacks. Access rules determine user rights to access data and limits user access to healthcare data [3] [8]. Access control policies are equally inescapable and crucial as encryption techniques for protecting patient privacy. There mainly three Access Control Mechanisms (ACMs) [1] [7] [24]: Role-based, Attribute-based, and Identity-based. In the Role-based Access Control Technique, roles are assigned to the system users to access private health data. Then it was later upgraded to include time-bounded functionalities for increasing the privacy and security of EHRs. Attribute-based Access Control uses cryptographic and non-cryptographic approaches. Cryptographic approaches are Ciphertext-Policy Attribute-Based Encryption (CP-ABE) and Key-Policy Attribute-Based Encryption (KP-ABE) [18]. The non-Cryptographic approach requires a trusted third party to carry the private keys and share the keys with the authorized users. The third access control method is Identity-Based Access Control (IBAC) which uses identity-based encryption (IBE) to employ users' identity information for encryption.

These approaches are static and conventional. They provide fine-grained access control and are suitable for the EHR requirements in normal situations. But cloud-based EHRs are complex and need to change access policies to consider on-demand user revocation and emergencies. Therefore, requires adaptive security to control unauthorized access to patient data [22] [27] [34].

Recent publications [22] [34] have proposed the inclusion of threat analysis by considering some conditions like the trust and risk level for granting/revoking user requests. The authors of [34] proposed a dynamic and adaptive security model, which interrogates trust parameters by measuring user behavior while accessing the EHR data. A user requests to access resources are controlled with an access control rule set managed through user behavior.

**4) Data Anonymization:**

Data Anonymization is used to protect the privacy of patient's data from cloud service providers, and malicious and unauthenticated insiders or outsiders. It keeps the patient's identity unidentified when records are released publicly for research. Anonymity means masking personally identifiable data such as aadhar number, name, address, date of birth from the health data contents [26]. Researchers have developed several anonymization techniques such as data masking,

pseudonymization, or de-identification [1]. These techniques are useful for ensuring data confidentiality from accidental data disclosure and provides the utmost privacy.

The first anonymization technique is data masking. It hides sensitive data elements with an anonymous value [3]. The disadvantage of data masking is, it permanently changes the original value. The second technique is pseudonymization. It removes all the identifiable data elements from the patient's dataset. These methods do not provide complete protection to the patient's private-sensitive information, and privacy is vulnerable even though attackers have minimum background knowledge of the algorithm. Forming an algorithm that efficiently preserves privacy is required to reduce the risk of re-identification [26].

There are many techniques such as k-anonymity, l-diversity, and t-closeness, initiated to enhance this traditional technique by increasing the privacy of patients. Identity disclosure is protected in k-anonymity but it fails to protect attribute disclosure. Hence, another property named p-sensitive anonymity was proposed to extend the k-anonymity, which safeguards both identities and attribute disclosure. L-diversity is group-based anonymization, utilized to preserve privacy in data sets. It utilizes generalization and suppression methods to reduce the granularity of data representation. T-closeness is a further advancement of l-diversity. These anonymizing methods face problems when data sets are high dimensional [3] [22] [27]. Therefore, there is a requirement for a hybrid technique to filter the healthcare data and limits the view of different users. For example, the authors of [33] proposed a privacy-preserving technique to prevent the sensitive healthcare database from linking and inference attack while restricting views of a database for illegitimate person impersonating as a valid user. They have combined query set size restriction and k-anonymity to filter the healthcare data and restrict the view of different users.

**5) Auditing and Monitoring:**

Auditing confirms the integrity of the healthcare records. Using an audit scheme, a cloud service provider can catch any abuses made to the system by unauthorized users [3]. Audit trails log all the EHR activities such as addition, modification, and deletion with the date and time stamp. This information would help locate and identify any form of misconduct that could affect EHR solutions [28].

Healthcare organizations must take measures to detect and prevent unauthorized access to EHR records [1]. There are some problems with the current auditing approach. Firstly, it increases storage requirements. Secondly, healthcare organizations conduct auditing and monitoring once a suspected privacy breach has taken place. Thirdly sometimes the information logged is not enough for proceeding analysis. Fourth, healthcare organizations are recording only authenticated user activities. Recent research suggests that lack of accountability is the major obstacle in the hindrance of cloud-based EHRs [22]. There is a need for healthcare organizations to address proactive and ongoing auditing and monitoring to prevent data breaches.

## 4. EHR Security and Privacy threats analysis in Cloud Environment

The usage of cloud-based EHR applications by healthcare organizations is growing enormously in the last ten years. The cloud threat spectrum for EHR applications has been increased so fast and could diminish patient trust towards EHR systems. This section focus on various threats associated with cloud-based EHR applications and associated solutions proposed by researchers. The healthcare service provider has to detect and prevent these threats since they can create serious harm to the EHRs.

**Threat 1: Insider Threat**

In this type of threat, a malicious insider accesses the healthcare records intentionally for causing harm to the patient or system. An insider could be a doctor, a nurse, or a former employee who misuse or abuse their privileges to perform unauthorized actions. These threats are much more dangerous than outsider attacks. Being a legitimate user of the system, they perform unauthorized and malicious actions without being caught or access rights revocation. Insider attacks are the most difficult to deal with since detection of them often occurs long after the damage has done [8].

Solution: There is a need for a dynamic and adaptive access control model which controls user access view by measuring risk factor based on their behavior (user trust). A technique which differentiates malicious masquerading behavior from legitimate access to the healthcare information system is needed. A profile for the authenticated user has to be maintained to compare user behavior against established user patterns. Numerous efforts have been made to detect insider threats, but concern regarding the achievement of higher accuracy levels remains an open challenge [29] [34].

**Threat 2: Abusive Use of Patients' Sensitive Data by Doctors during Emergency Cases**

Healthcare organizations allow doctors to override access permission during emergency situations also known as the break-the-glass (BTG) approach. The normal work-flow of the healthcare system gets violated in BTG situations. This BTG approach opens the door for doctors or other staff members to exploit or disclose patient's personal information without the patient's consent. Health service providers are maintaining logs to protect against intentional or accidental information misuses. The current approach is preventive and not adequate for the BTG situations [8] [28].

Solution: There should be patient-centric information accountability and transparency. The health service provider should maintain a system activity log so the patient can detect potential vulnerabilities to their sensitive data and incident responses through revoking authorization on their health data [22]. If a doctor or any internal user breaches a patient's confidentiality, then rights should be dismissed [28]. A revoked person cannot access future EHRs even if his previous role satisfies the access policy [1].

**Threat 3: Masquerade Attack**

In this type of threat, a attacker masquerades as a legitimate user and performs unauthorized access to the system. An attacker can be hacker or malicious insider who has stolen an identity of an authenticated user. Masquerade attacker can utilize all of the user's privileges to access sensitive information of a patient. This type of threats are difficult to detect due to the trust imparted to compromised user accounts [8]. To protect information systems from unauthorized use, administrators rely on security technologies such as firewalls, network-based intrusion detection systems, and strong authentication protocols but if an attacker has gained access to a legitimate user account, these state-of-the-art security technologies are rendered useless [29].

Solution: The masquerade attack is a dangerous threat to the security of information systems due to its ability to completely undermine security technologies. There is a requirement for a model which can detect masquerade attack by estimating the amount of risk in user data access request [22]. However, risk-based access control methods are new and have not been given much consideration.

**Threat 4: Outsider Intrusion**

Hackers, network intruders, previous employees, or others may steal or access information, disrupt operations, and damage systems. This threat is a pure technical threat where an attacker cracks into a healthcare system through an outer network and acquires patient records. Therefore, it is an untapped problem on the horizon [8].

Solution:
It is difficult to identify outsider's intrusion because they illegally access the system. A system needs to verify whether the data received from a legitimate user, preventing unauthorized entities from injecting information into the system's database [30]. The system should use identity management and behavior-based access control policy to recognize fraudulent transactions of outsiders.

**Threat 5: Data breaches during an accidental disclosure**

Healthcare organizations experience frequent shifting of staff members. Also, healthcare data are accessed by many stakeholders with different access privileges according to their role [18]. Managing different settings for each user cannot be handled by existing access control models. They are static and may conflict in handling dynamic attributes of users and resources in healthcare organizations. The diversity of the services and dynamic allocation of the resources generate overlapping in policies results in data leakages to unintended or illegitimate users [8]. The data breaches damage extent depends on the sensitivity of breached information.

Solution: Many attempts have been tried for restricting data breaches, yet a solution has not been found, remains an open challenge.

**Threat 6: Uncontrolled secondary usage**

Healthcare organizations collect patient information to provide primary care and ensure that it should not be utilized for any other purpose not mentioned in the contract. For instance, for different research agendas, for example, disease tracking by producing a national medical data repository from the information assembled from general professionals and other care deliverers [31]. A hacker or an attacker may steal or hack this data repository for their benefit which, threatens the integrity of EHRs.

Solution: Many attempts have been made at detecting these attacks, yet a solution is not been found and it remains an open challenge.

## 5. Discussion

**Open Research Challenges**

Many healthcare organizations around the world are adopting cloud-based EHR applications to find innovative solutions for stakeholders. However, there are many security and privacy concerns that hindrance to wide adoption of cloud-based EHRs. The cloud service providers perform various data security and privacy mechanisms such as encryption, digital signature, access control, authentication exchange, and audit. Fundamentally, all these techniques are focused on preserving patient's privacy and security and are lacking in the transparency and accountability of the data accessed.

Many open issues are present that are required to be solved for providing reliable and protected cloud infrastructure. The first open issue is regarding sharing of patient health records between many stakeholders of the same or different healthcare organizations. The EHR systems should have a different setting and different access rights for each user according to their roles. The healthcare system is complex and used by various stakeholders requires a dynamic access control policy. With an existing access control policy, dynamic allocation of the resources is difficult, especially in emergencies when the system allows the doctors to inherit privileges from lower roles or allows emergency functionality. In such cases if doctors misuses the information then they should be traced by the system. Therefore, there is a need for a transparent system where each transaction should be traceable and auditable to control data access and detect malicious transactions.

Cloud computing also needs a security solution against the insider threat. In this attack, a hacker takes on the credentials of a legitimate person to perform unauthorized actions. Insider attacks are the most difficult to detect as an attacker utilizes all the privileges of an authorized user to bypass all the safeguards. Therefore, in this scenario, there is a need to develop an indicator that can help to detect the insider attack by comparing user activity against generated log patterns. There is a need to apply adaptive authentication model which allows access to the resources based on user pattern by measuring risk factor besides two-factor authentication. Also, the system should implement a on-demand or forward revocation mechanism that restricts revoked users to access the future EHRs. Numerous attempts have been made but not sufficient to solve and achieving high levels of accuracy remains an open challenge. Similarly, identifying who is the legitimate user and who is the illegitimate user is yet another problem faced by cloud-based EHR systems.

Cloud-based EHR applications have brought numerous benefits for healthcare providers and patients although, they expose threats to data security and privacy. The success and acceptance of cloud-based EHR services rely on the level of security provided.

**Evaluation of the Existing EHR Frameworks with Respect to the Security and Privacy Requirements**

**Table 1**

**Comparative analysis of the related works.**

| Framework | IN | CO | AU | NR | AC | AN | CE | PC | AA | References |
|---|---|---|---|---|---|---|---|---|---|---|
| A Secure Framework for Sharing Electronic Health Records over Clouds | Y | Y | Y | Y | N | N | N | Y | N | [36] |
| Authentication and Access Control in e-Health Systems in the Cloud | - | Y | Y | Y | - | Y | N | N | N | [37] |
| Security and privacy preserving approaches in the eHealth clouds with disaster recovery plan | Y | Y | Y | Y | N | - | Y | N | N | [38] |
| User Authentication Algorithm with Role-Based Access Control for Electronic Health Systems to Prevent Abuse of Patient Privacy | Y | Y | Y | Y | Y | - | N | N | N | [39] |
| Continuous and Transparent Access Control Framework for Electronic Health Records: A Preliminary Study | Y | Y | Y | Y | Y | - | Y | Y | Y | [22] |
| Preserving confidentiality and privacy of the patient's EHR using the OrBAC and AES in cloud environment | Y | Y | Y | N | N | N | Y | N | N | [40] |
| Delegated Authorization Framework for EHR Services using Attribute Based Encryption | Y | Y | Y | Y | N | N | N | N | N | [25] |
| A Secure Access Control Model for E-health Cloud | - | Y | Y | N | N | N | N | N | Y | [34] |

*** Requirements legends -- IN: Integrity; CO: Confidentiality; AU: Authenticity; NR: Non-Repudation; AU: Accountability; AN: Anonymity; CE: Consent Exception; PC: Patient's Control; AA: Adaptive Authentication.**
**Three options for assessments -- Y: Specific requirement is covered; N: Specific requirement is not covered; --: Specific requirement is not discussed.**

Here we have given a comparative view of some relevant works related to cloud security and privacy requirements for healthcare systems in Table 1. The security requirements that were addressed in this work were as follows: data confidentiality, authenticity, non-repudation, accountability, anonymity, consent exception, patient's control, and adaptive authentication (trust-based by measuring risk). We have noticed that all such solutions use static access structures to define access control policies that are not appropriate with the dynamic environment of cloud-based EHRs. Furthermore, they have not focused on accountability, patient' control, consent exception, and adaptive authentication.

Most of the existing studies have shown accountability on the administrator side but have not focused on patient data transparency. Some of them proposed the framework that patients can control the right of their health records.

Incorporating accountability of EHRs provides non-restrictive access to authorized persons while health information would not be misused. Accountability helps in tracking transactions by maintaining a log of the transactions. Healthcare providers must inform the patient when there has been a violation of privacy. All the transactions should be transparent and traceable for maintaining the security, privacy, and integrity of data on cloud servers. This approach could help detect unauthorized access and illegal disclosure of healthcare records by authorized and unauthorized users.

The healthcare data are strictly confidential and stored on cloud servers, require additional security and safety for the records besides two-factor authentication. The existing security and privacy protection mechanisms will not be adequate and effective to address increased threat vectors. Employing user pattern-based adaptive and continuous authentication will provide more protection from threats without user intervention. There is a need for an approach that streamlines the sharing of medical records in a secure way, protects sensitive data from hackers, and gives patients more control over their information.

## 5. Conclusion

The cloud-based EHR preserves patient's medical information for various purposes such as easy sharing of records between stakeholders, accurate treatment of patients, real-time monitoring, medical data analysis, etc. However, outsourcing private medical data on a third-party server has a dangerous impact on data integrity, privacy, and security. Security and privacy concerns become more challenging in real-time healthcare services because threats to the EHR can lead to wrong medication and puts patient's life in danger. Numerous works have been done to secure healthcare data using encryption or digital signature and fine-grained access control in the cloud environment. Existing information security mechanisms are helpful to some extent but cannot guarantee absolute security. Available evidence suggests traditional access control approaches cannot adequately protect patient's sensitive data from potential adversaries. Therefore, there is a need for secure and efficient data access mechanism which can protect EHRs against insider and outsider threats. Implementing a Blockchain-based distributed ledger for the cloud-based EHR applications can figure out security issues and protect the privacy of patients. In the future, we will try to combine blockchain with a cloud platform to provide transparency and accountability to the distributed EHR systems to resist insider attacks. We will also focus on trust-based self-adaptive security by measuring risk while making access decisions for users.

## References

[1] Chenthara, S., Ahmed, K., Wang, H., & Whittaker, F. (2019). Security and privacy-preserving challenges of e-health solutions in cloud computing. IEEE access, 7, 74361-74382.
[2] Office of the National Coordinator for Health Information Technology. 'Office-based Physician Electronic Health Record Adoption,' Health IT Quick-Stat #50. dashboard.healthit.gov/quickstats/pages/physician-ehr-adoption-trends.php. January 2019.
[3] Abouelmehdi, K., Beni-Hessane, A., & Khaloufi, H. (2018). Big healthcare data: preserving security and privacy. Journal of Big Data, 5(1), 1.
[4] M. D. Forecast, "Cloud Computing Market," Market Data Forecast, September 2020. [Online]. Available: https://www.marketdataforecast.com/market-reports/cloud-computing-market. [Accessed December 2020].
[5] Tanwar, S., Tyagi, S., & Kumar, N. (2019). Security and Privacy of Electronic Healthcare Records. Institution of Engineering and Technology. https://doi.org/10.1049/PBHE020E
[6] Al-Issa, Y., Ottom, M. A., & Tamrawi, A. (2019). EHealth Cloud Security Challenges: A Survey [Abstract]. Journal of Healthcare Engineering, 2019, 1-15. doi:10.1155/2019/7516035
[7] Rana, M. E., Kubbo, M., & Jayabalan, M. (2017). Privacy and Security Challenge towards Cloud-Based Access Control. Asian. Journal of Information Technology, 16(2-5), 274-281.
[8] For the record: Protecting electronic health information. (1997). Washington, D.C: National Academy Press. Doi: 10.17226/5595
[9] Chukwu, E., & Garg, L. (2020). A systematic review of blockchain in healthcare: Frameworks, prototypes, and implementations. IEEE Access, 8, 21196-21214.
[10] Rezaeibagha, F., Win, K. T., & Susilo, W. (2015). A Systematic Literature Review on Security and Privacy of Electronic Health Record Systems: Technical Perspectives. Health Information Management Journal, 44(3), 23-38. doi:10.1177/183335831504400304
[11] Walker-Roberts, S., Hammoudeh, M., & Dehghantanha, A. (2018). A Systematic Review of the Availability and Efficacy of Countermeasures to Internal Threats in Healthcare Critical Infrastructure. IEEE Access, 6, 25167-25177.
[12] S. Coble, "Report Reveals Worst State for Healthcare Data Breaches in 2019," Inforsecurity Group, 14 February 2020. [Online]. Available: https://www.infosecurity-magazine.com/news/Report Reveals Worst State for Healthcare Data Breaches in 2019. [Accessed December 2020].

[13] D. Palmer, "Cybersecurity: This password-stealing hacking campaign is targeting governments around the world," ZDNet, 12 December 2019. [Online]. Available: https://www.zdnet.com/article/ cybersecurity-this-password-stealing-hacking-campaign-is-targeting-governments-around-the-world/. [Accessed December 2020].
[14] HIPPA JOURNAL, "Key Findings of the 2019 Verizon Data Breach Investigations Report," HIPPA JOURNAL, 8 May 2019. [Online]. Available: https:// www.hipaajournal.com/ 2019-verizon -data-breach-investigations-report-findings/. [Accessed December 2020].
[15] Farhadi, M., Haddad, H., & Shahriar, H. (2018, July). Static Analysis of HIPPA Security Requirements in Electronic Health Record Applications. In 2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC) (Vol. 2, pp. 474-479). IEEE.
[16] Azeez, N. A., & Van der Vyver, C. (2019). Security and privacy issues in e-health cloud-based system: A comprehensive content analysis. Egyptian Informatics Journal, 20(2), 97-108.
[17] Hossain, M. A., Hossain, M. B., Uddin, M. S., and Imtiaz, S. M. (2016). Performance Analysis of Different Cryptography Algorithms. International Journal of Advanced Research in Computer Science and Software Engineering, 6(3).
[18] Kamoona, M. A., & Altamimi, A. M. (2018, July). Cloud E-health Systems: A Survay on Security Challenges and Solutions. In 2018 8th International Conference on Computer Science and Information Technology (CSIT) (pp. 189-194). IEEE.
[19] Al Hamid, H. A., Rahman, S. M. M., Hossain, M. S., Almogren, A., & Alamri, A. (2017). A security model for preserving the privacy of medical big data in a healthcare cloud using a fog computing facility with pairing-based cryptography. IEEE Access, 5, 22313-22328.
[20] Chandravathi, D., & Lakshmi, P. V. Performance Analysis of Homomorphic Encryption algorithms for Cloud Data Security.
[21] Gulsezim, D., Zhansaya, S., Razaque, A., Ramina, Y., Amsaad, F., Almiani, M., & Oun, A. (2019, October). Two Factor Authentication using Twofish Encryption and Visual Cryptography Algorithms for Secure Data Communication. In 2019 Sixth International Conference on Internet of Things: Systems, Management and Security (IOTSMS) (pp. 405-411). IEEE.
[22] Jayabalan, M., & Oadaniel, T. (2017). Continuous and transparent access control framework for electronic health records: A preliminary study. 2017 2nd International Conferences on Information Technology, Information Systems and Electrical Engineering (ICITISEE). doi:10.1109/icitisee.2017.8285487
[23] M. Jayabalan, T. O'Daniel (2019). A study on authentication factors in Electronic Health Records. Journal of Applied Technology and Innovation, vol. 3, no. 1, pp. 7–14.
[24] Yüksel, B., Küpçü, A., & Özkasap, Ö. (2017). Research issues for privacy and security of electronic health services. Future Generation Computer Systems, 68, 1-13. doi:10.1016/j.future.2016.08.011
[25] Joshi, M., Joshi, K. P., & Finin, T. (2019). Delegated authorization framework for EHR services using attribute based encryption. IEEE Transactions on Services Computing.
[26] Tasatanattakool, P., & Techapanupreeda, C. (2017, December). User authentication algorithm with role-based access control for electronic health systems to prevent abuse of patient privacy. In 2017 3rd IEEE International Conference on Computer and Communications (ICCC) (pp. 1019-1024). IEEE.
[27] Sahi, M. A., Abbas, H., Saleem, K., Yang, X., Derhab, A., Orgun, M. A., Yaseen, A. (2018). Privacy Preservation in e-Healthcare Environments: State of the Art and Future Directions. IEEE Access, 6, 464-478. doi:10.1109/access.2017.2767561
[28] Wickramage, C., Fidge, C., Sahama, T., & Wong, R. (2017, December). Challenges for log based detection of privacy violations during healthcare emergencies. In GLOBECOM 2017-2017 IEEE Global Communications Conference (pp. 1-6). IEEE.
[29] Shaikh, V., Pattanshetti, P., & Tanuja, R. (2019). Detection of Insider Attack in Distributed Systems. Detection of Insider Attack in Distributed Systems (May 18, 2019).
[30] Premarathne, U., Abuadbba, A., Alabdulatif, A., Khalil, I., Tari, Z., Zomaya, A., & Buyya, R. (2016). Hybrid cryptographic access control for cloud-based EHR systems. IEEE Cloud Computing, 3(4), 58-64.
[31] Pussewalage, H. S. G., & Oleshchuk, V. A. (2016). Privacy preserving mechanisms for enforcing security and privacy requirements in E-health solutions. International Journal of Information Management, 36(6), 1161-1173.
[32] Kumar, R., & Goyal, R. (2019). On cloud security requirements, threats, vulnerabilities and countermeasures: A survey. Computer Science Review, 33, 1-48.
[33] Kundalwal, M. K., Chatterjee, K., & Singh, A. (2019). An improved privacy preservation technique in health-cloud. ICT Express, 5(3), 167-172.
[34] Singh, A., Chandra, U., Kumar, S., & Chatterjee, K. (2019, October). A Secure Access Control Model for E-health Cloud. In TENCON 2019-2019 IEEE Region 10 Conference (TENCON) (pp. 2329-2334). IEEE.
[35] Goyal, V., & Kant, C. (2018). An effective hybrid encryption algorithm for ensuring cloud data security. In Big Data Analytics (pp. 195-210). Springer, Singapore.
[36] Ibrahim, A., Mahmood, B., & Singhal, M. (2016, May). A secure framework for sharing electronic health records over clouds. In 2016 IEEE International Conference on Serious Games and Applications for Health (SeGAH) (pp. 1-8). IEEE.
[37] Kahani, N., Elgazzar, K., & Cordy, J. R. (2016, April). Authentication and access control in e-health systems in the cloud. In 2016 IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS) (pp. 13-23). IEEE.
[38] Sahi, A., Lai, D., & Li, Y. (2016). Security and privacy preserving approaches in the eHealth clouds with disaster recovery plan. Computers in biology and medicine, 78, 1-8.

[39] Tasatanattakool, P., & Techapanupreeda, C. (2017, December). User authentication algorithm with role-based access control for electronic health systems to prevent abuse of patient privacy. In 2017 3rd IEEE International Conference on Computer and Communications (ICCC) (pp. 1019-1024). IEEE.
[40] Babrahem, A. S., & Monowar, M. M. (2018). Preserving confidentiality and privacy of the patient's EHR using the OrBAC and AES in cloud environment. International Journal of Computers and Applications, 1-12.

**First Author: Prof. Vidhi Thakkar is currently working as an assistant professor at GLS University, Ahmedabad, Gujarat, India. She has completed her masters in Computer Applications from GTU. Her area of interest are Cloud computing security and privacy and blockchain.**

**Second Author: Dr. Vrushank Shah, Deputy Director, Indus Center for Startups, Incubation and Innovation and Head, Electronics and Communication, Indus University, Ahmedabad. He has more than 12 years of academic experience and have published more than 13 papers in peer reviewed journals. Dr Shah is reviewer in many peer reviewed journals in the area of computer networking. His areas of interests include data mining, network security, communication and signal processing systems.data mining, network security, communication and signal processing systems.**